



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,914	03/26/2001	W. Dale Hopkins	20206-16 (P00-3324)	4267

22879 7590 03/02/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

CALLAHAN, PAUL E

ART UNIT PAPER NUMBER

2137

DATE MAILED: 03/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/818,914	Applicant(s) HOPKINS ET AL.	
	Examiner Paul Callahan	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 November 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 7-16, 18-26, 28, 29, 31-36, 38-46, 48-52, 54-56 and 59-66 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 24-26, 28, 29, 31-36, 38-46, 48-52, 65 and 66 is/are allowed.
- 6) ☒ Claim(s) 1, 5, 7, 8, 12, 13, 15, 16, 18, 19, 21, 22, 26, 54, 63 and 64 is/are rejected.
- 7) ☒ Claim(s) 2-4, 8-11, 14, 19, 20 and 23 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ <u>PTC 2-12-06</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11-30-05 has been entered.

Claims 1-63 were pending in this application at the time of the previous Office Action. Claims 6, 17, 27, 30, 37, 47, 53, 57, and 58 have been cancelled and new claims 64-66 added by the amendment filed 11-30-05. Therefore claims 1-5, 7-16, 18-26, 28, 29, 31-36, 38-46, 48-52, 54-56, and 59-66 are now pending and have been examined.

Response to Arguments

2. Applicant's arguments with respect to claims 1-5, 7-16, 18-26, 28, 29, 31-36, 38-46, 48-52, 54-56, and 59-66 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

Art Unit: 2137

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 8, 19, 26, 63, and 64 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim contains the passage: "...testing the relative primality of each said prime number candidate minus one and said specified public exponent e ..." It is unclear whether the applicant intends the passage to read as testing all but one of the plurality of candidates, or to be read as subtracting the number one from each candidate value and then testing it. Additionally, from the passage it is not clear if the applicant intends to have the value of each candidate reduced by the number one, or reduced by the number one and also by the additional amount represented by the specified public exponent e , and then tested, or if the candidate value minus the number one is to be tested for primality, with the public exponent e then tested for primality separately.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 5, 7, 12, 13, 15, 16, 18, 21, 22, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handbook of Applied Cryptography, Menezes et al., CRC Press 1996, pages 134-168, and Kent White, "Experiments in Parallel Processing for Undergraduate Students" 29th ASEE/IEEE Frontiers in Education Conference, pp. 11a3-1-11a3-4, Nov. 10-13-1999, and Daniel M. Gordon, "A Survey of Fast Exponentiation Methods", Journal of Algorithms 27, pp. 129-146, 1998.

As for claims 1, 5, and 12, Menezes teaches a process of searching for a plurality of prime number values, comprising the steps of: randomly generating a plurality of k random odd numbers each providing a prime number candidate (Sec. 4.1.1, p. 134); and performing a plurality of t primality tests on each of the plurality of k randomly generated prime number candidates (Sec. 4.1.1, p. 134), each of the plurality of $(k \times t)$ primality tests including an associated exponentiation operation (Sec. 4.2.1: Fermat's Test p. 136, Sec. 4.2.3: Miller-Rabin Test p. 138-140). Menezes does not teach a processing system including a processing unit and a plurality $(k \times t)$ of exponentiation units communicatively coupled to the processing unit, or that the primality tests are carried out by the plurality of exponentiation units in parallel and where the exponentiation operations are carried out simultaneously. However White teaches such a parallel arrangement of processors carrying out primality testing simultaneously (fig. 1, page 11a3-1, Sec. I: Introduction, Sec. III. Version One, Sec. IV Version Two). White fails to teach that the primality test utilized involved processor exponentiation, however Gordon teaches that such an exponentiation step is utilized in most computer arithmetic logic units (algebra systems). For example, where Fermat's test for primality is commonly used in prime number generation. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate

these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claim 7, Menezes teaches sieving prime number candidates by performing a small divisor test on each of said candidates in order to eliminate candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number s of candidates (Page 145, Sec. 4.4.1); and performing at said plurality of t primality tests on each of said sieved number s of candidates (Page 148, Sec. 4.5.1), each of the plurality of s primality tests including an associated exponentiation operation (Page 146, Sec 4.4.1). Menezes does not teach a processing system including a processing unit and a plurality st of exponentiation units communicatively coupled to the processing unit, or that the primality tests are carried out by the plurality st of exponentiation units in parallel and where the exponentiation operations are carried out simultaneously. However White teaches such a parallel arrangement of processors carrying out primality testing simultaneously (fig. 1, page 11a3-1, Sec. I: Introduction, Sec. III. Version One, Sec. IV Version Two). White fails to teach that the primality test utilized involves processor exponentiation, however Gordon teaches that such an exponentiation step is utilized in most computer arithmetic logic units (algebra systems), for example where Fermat's test for primality is used in prime number generation. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claim 13, Menezes teaches a step of performing at least one primality test that includes performing a Miller-Rabin type primality test (Sec. 4.2.3).

As for claims 15, 21, and 22, Menezes teaches a process of searching for a plurality of prime number values comprising the steps of: randomly generating at least one random odd number providing a prime number candidate (sec. 4.1.1); determining a plurality of y additional odd numbers based on said at least one randomly generated odd number to provide y additional prime number candidates (sec. 4.1.1: sequence is created by generating a random odd n , and using it as a seed for the creation of a plurality of odd numbers: $n+2, n+4, n+6, \dots$), thereby providing a total number of $y+1$ candidates (sec. 4.1.1); performing a plurality t of primality tests on each of said $(y+1) \times t$ candidates (sec. 4.2.1: Fermat's test, sec. 4.2.3: Miller-Rabin test), each of the $(y+1) \times t$ primality tests including an associated exponentiation operation (sec. 4.2.3.). White teaches a plurality of $(y + 1) \times t$ processors communicatively coupled with a central processing unit, carrying out a plurality t of primality tests, executed simultaneously by an associated one of the $(y+1) \times t$ of the processing units. White does not teach said primality tests as being performed by exponentiation. However Gordon teaches that primality testing by processors carrying out exponentiation (Sec. I: Introduction p. 129). Gordon teaches that such primality testing by Fermat's test using exponentiation is common in processor arithmetic logic units (computer algebra systems). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claim 16, Menezes teaches a prime number generating system wherein said step of determining a plurality of y additional odd numbers based on at least one of the randomly generated odd numbers, expressed as $n_{o,o}$, includes successively adding two to it in order to provide $(y + 1)$ additional prime number candidates expressed as (Page 148, Sec. 4.5.1).

As for claim 18, Menezes teaches sieving prime number candidates by performing a small divisor test on each of said $(y + 1)$ candidates in order to eliminate candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number of candidates (Page 145, Sec. 4.4.1)

As for claim 54, the claim is directed towards the computer program product, embodied in a memory medium, that when read out cause the computer to carry out the method of claim 1. Therefore the claim is rejected on the same basis as is claim 1.

Allowable Subject Matter

7. Claims 24, 25, 28, 29, 31-36, 38-46, 48-52, 55, 56, 59-62, 65, and 66 are allowed.
8. Claims 2-4, 9-11, 14, 20, and 23 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The closest prior art in the field, Menezes, White and Gordon, does not teach the features of following claims:

As for claims 2, 45, 55: the determination of an additional plurality y of odd numbers for primality testing, the determination based on each of the plurality of k randomly generated odd numbers, resulting in a total number of $(k \times (y + 1) \times t)$ candidates, all in combination with the other claim limitations;

As for claims 10, 20, 24, 28, 59, 61, and 65: the performing of an additional $t-1$ additional plurality tests on a number of r candidates obtained by the applicant's small divisor sieving process and a first round t of plurality tests;


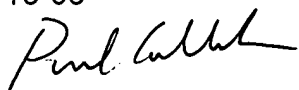
As for claims 14 and 23: the step of randomly generating that is performed over the interval L defined for each plurality k of random odd numbers and generating each of plurality k in a interval 2^L and 2^{L-1} .

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

2-16-06



MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137